EasyLock

Versión del Manual de Usuario 2.0.0.0

Manual de Usuario

Índice

1. Introducción

La protección de los datos en tránsito es esencial para asegurar que ningún tercero no tenga acceso a los datos en caso de que se pierde un dispositivo, es extraviado o robado. EasyLock permite a los dispositivos portátiles a identificarse como TrustedDevices (en combinación con Endpoint Protector) y protege los datos en el dispositivo con el modo de encriptación de 256 bits AES CBC, aprobado por el Gobierno.

Con la intuitiva interfaz Arrastrar y Soltar, los archivos se pueden copiar rápidamente hacia y desde el dispositivo para el flujo de trabajo rápido, seguro y eficiente.

EasyLock es una aplicación portable que no requiere ningún proceso de instalación en el PC host y siempre es portátil. A donde sea que el dispositivo de almacenamiento portátil va, EasyLock se guarda en el dispositivo y se puede utilizar en cualquier ordenador Windows, MAC o Linux.

2. Requisitos del sistema

Sistemas Operativos:

Windows 7 (todas las versiones)

Windows Vista (todas las versiones)

Windows XP (Service Pack 2 se recomienda)

Mac OS 10.5 o posterior

Linux - openSUSE 11.2 (otras distribuciones pueden estar disponibles bajo demanda)

Puerto USB disponible

Dispositivo de almacenamiento USB extraíble para iniciar la aplicación de (por ejemplo, la unidad flash USB, disco duro externo, tarjeta de memoria, etc.)

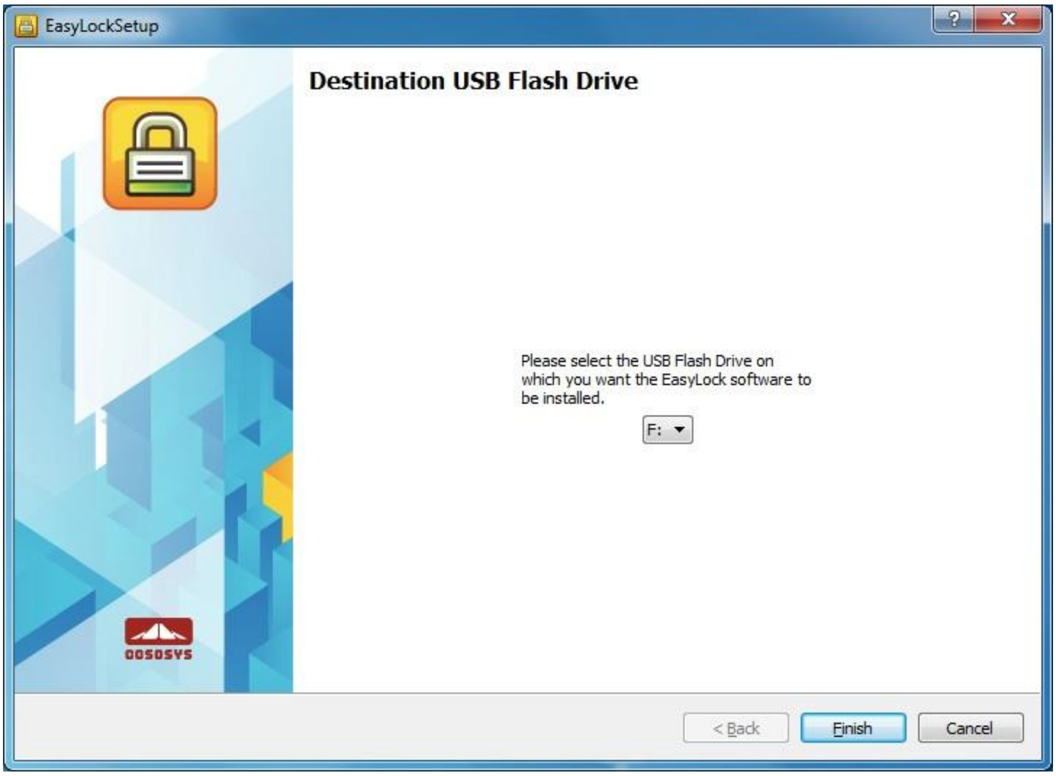
Si el dispositivo de almacenamiento portátil tiene un interruptor de protección contra escritura manual (bloqueo), debe ser en la posición desprotegida (de escritura) para ser capaz de utilizar EasyLock.

EasyLock no requiere derechos de administrador.

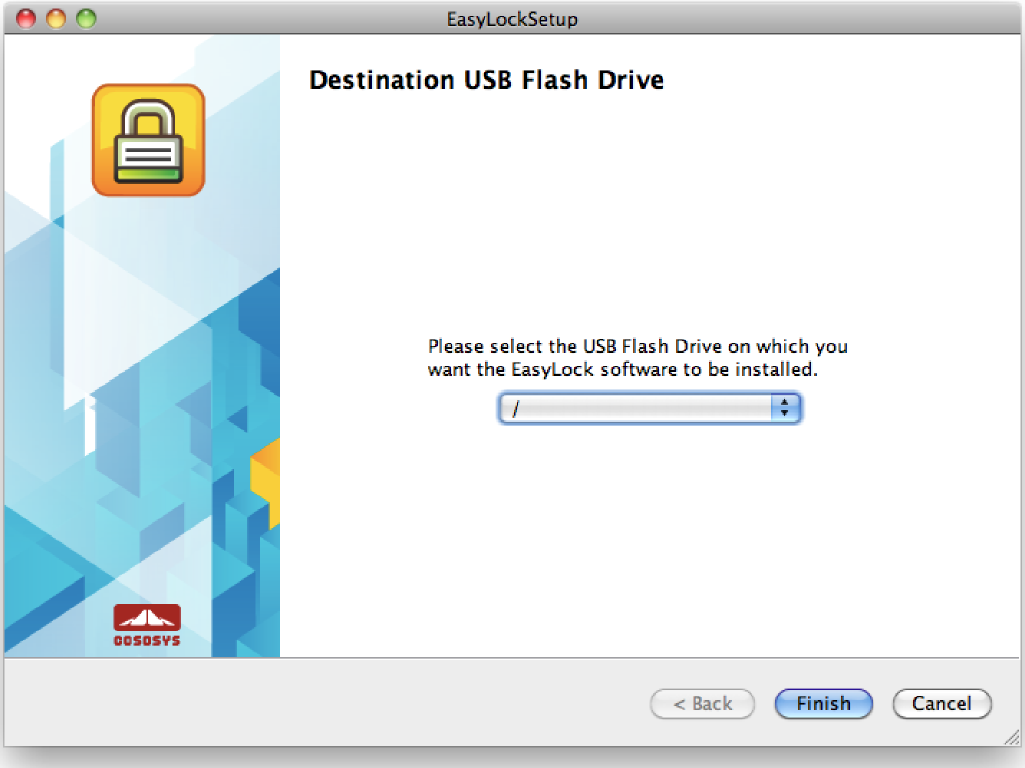
3. Instalación

Para instalar EasyLock en una unidad flash USB (u otro dispositivo de almacenamiento portátil USB):

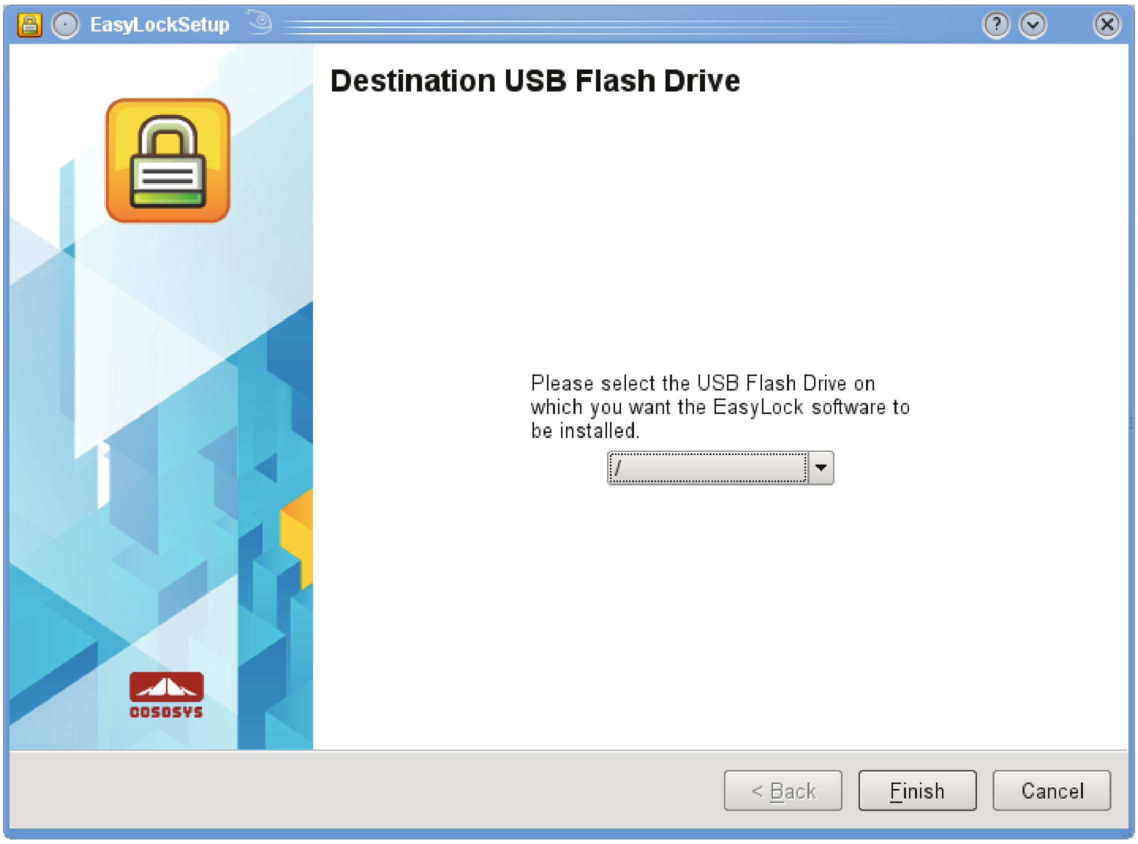
- **El sistema operativo Windows**: ejecute el archivo "EasyLockSetup.exe", seleccione la letra de unidad correspondiente al dispositivo USB y pulse <Finalizar>. La aplicación EasyLock se instalará automáticamente en la Carpeta raíz del dispositivo seleccionado.



- **En MAC OS**: ejecute el archivo "EasyLockSetup.dmg", seleccione la letra de unidad correspondiente al dispositivo USB y pulse <Finalizar>. La aplicación EasyLock se instalará automáticamente en la Carpeta raíz del dispositivo seleccionado.



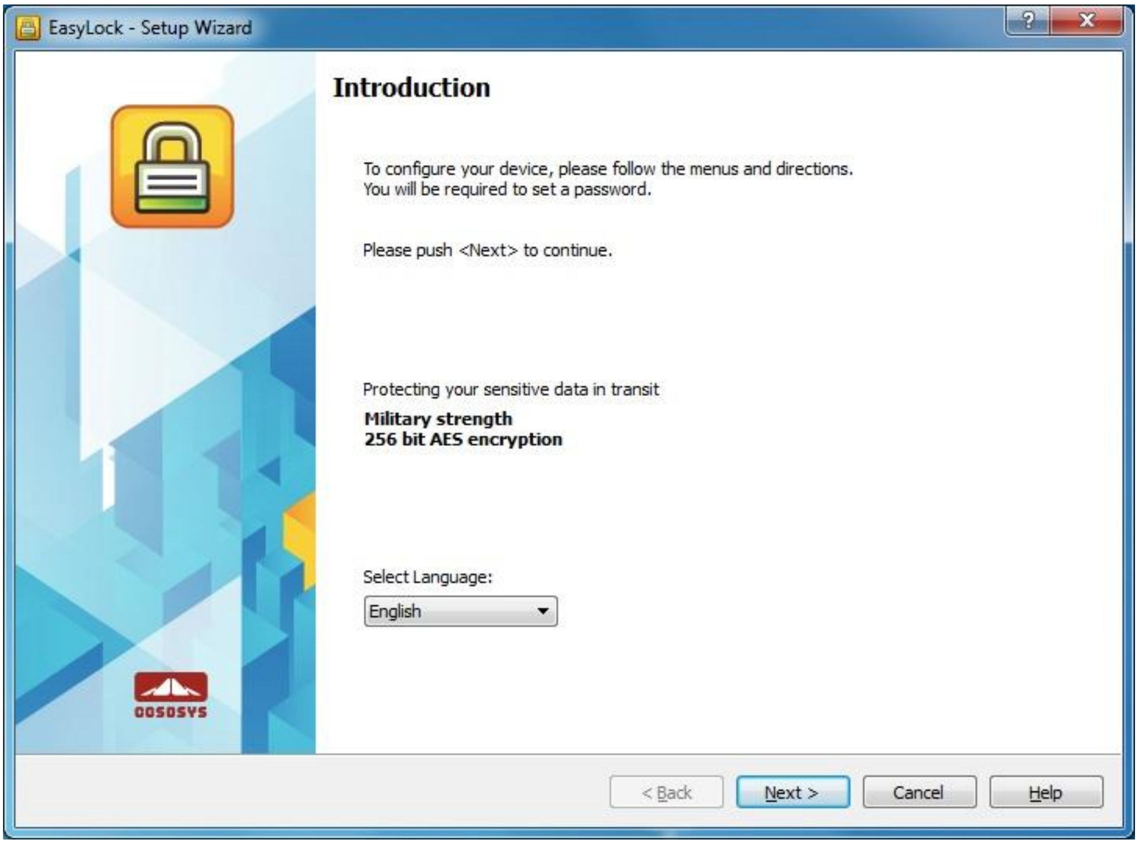
- **El sistema operativo Linux**: ejecute el archivo EasyLockSetup, seleccione la letra de unidad correspondiente al dispositivo USB y pulse <Finalizar>. La aplicación EasyLock se instalará automáticamente en la Carpeta raíz del dispositivo seleccionado.



3.1. Configuración de EasyLock

Para empezar EasyLock, simplemente haga doble clic en el archivo EasyLock que se guarda en la carpeta raíz del dispositivo de almacenamiento portátil.

Cuando se utiliza el dispositivo de almacenamiento portátil como un TrustedDevices en combinación con Endpoint Protector, el PC del cliente al que está conectado el dispositivo debe haber recibido la autorización del servidor Endpoint Protector, de lo contrario el dispositivo no se podrá acceder a un PC protegido por Endpoint Protector o EasyLock no iniciará automáticamente.



3.2. Configuración de una contraseña

Para la seguridad (encriptación) de datos, debe configurar una contraseña. La contraseña debe contener por lo menos 6 (seis) caracteres.

Por razones de seguridad, debe usar letras, números y símbolos en su contraseña.



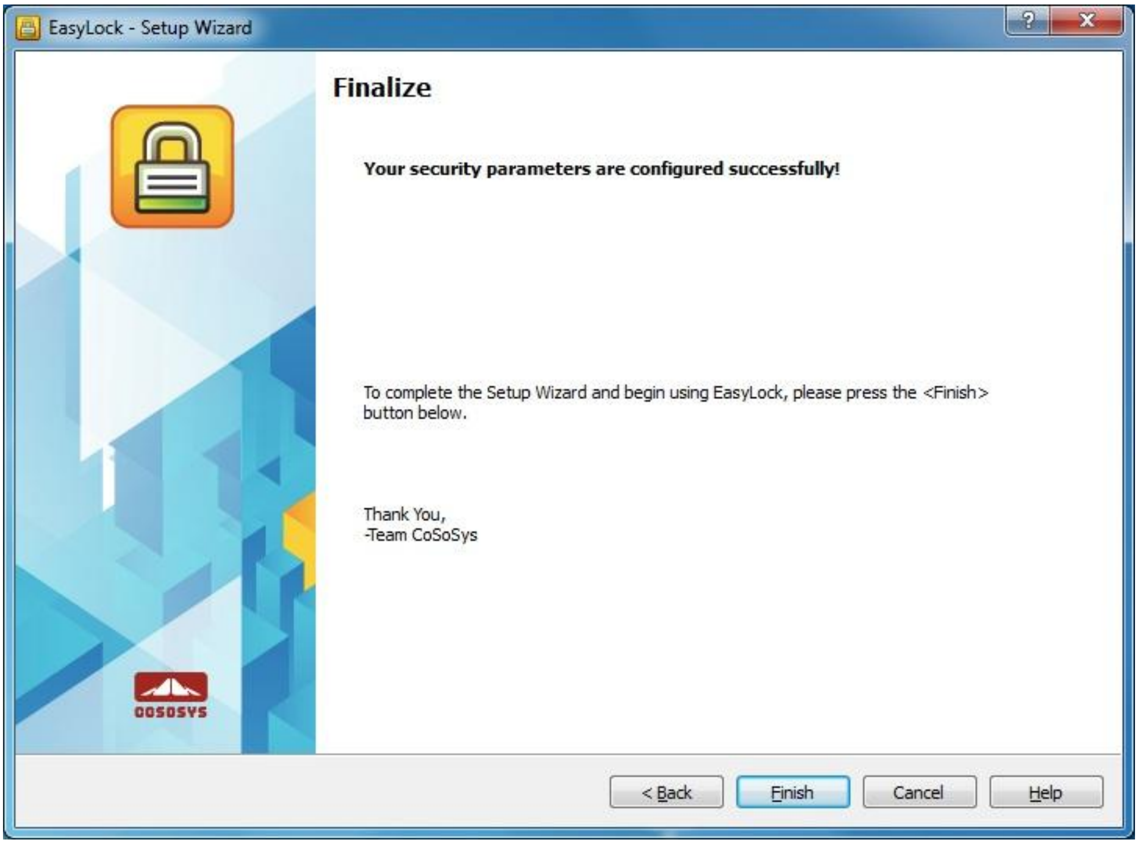
Introduzca la contraseña y luego confírmela.

También debe configurar un recordatorio de contraseña que le ayudará si usted olvida su contraseña.

Haga clic en "Siguiente" para continuar.



Haga clic en "Finalizar" para finalizar la configuración de la contraseña y para empezar a utilizar la aplicación.



3.3. Reintroducción de contraseña

Cada vez que se inicia la aplicación, se le pedirá, por razones de seguridad, para introducir su contraseña.

Para el caso de que la unidad se pierde o es robada, el número de reintentos de introducir la contraseña es limitado a 10 (diez). Después de que la contraseña se ha introducido erróneamente 10 (diez) veces consecutivas, EasyLock eliminará de una forma segura todos los archivos encriptados guardados en el dispositivo de almacenamiento portátil.

Los datos del dispositivo de almacenamiento portátil no pueden después ser recuperados o reconstruidos. Los datos son eliminados de forma permanente.

3.4. Configuración de la pantalla

En la barra de herramientas de EasyLock, hay dos diferentes opciones disponibles para personalizar la ventana de visualización de EasyLock.



Cambiar Paneles - para cambiar la pantalla del panel de la unidad USB con el panel Mi PC

Mostrar u ocultar el panel Mi PC - para mostrar el panel Mi PC

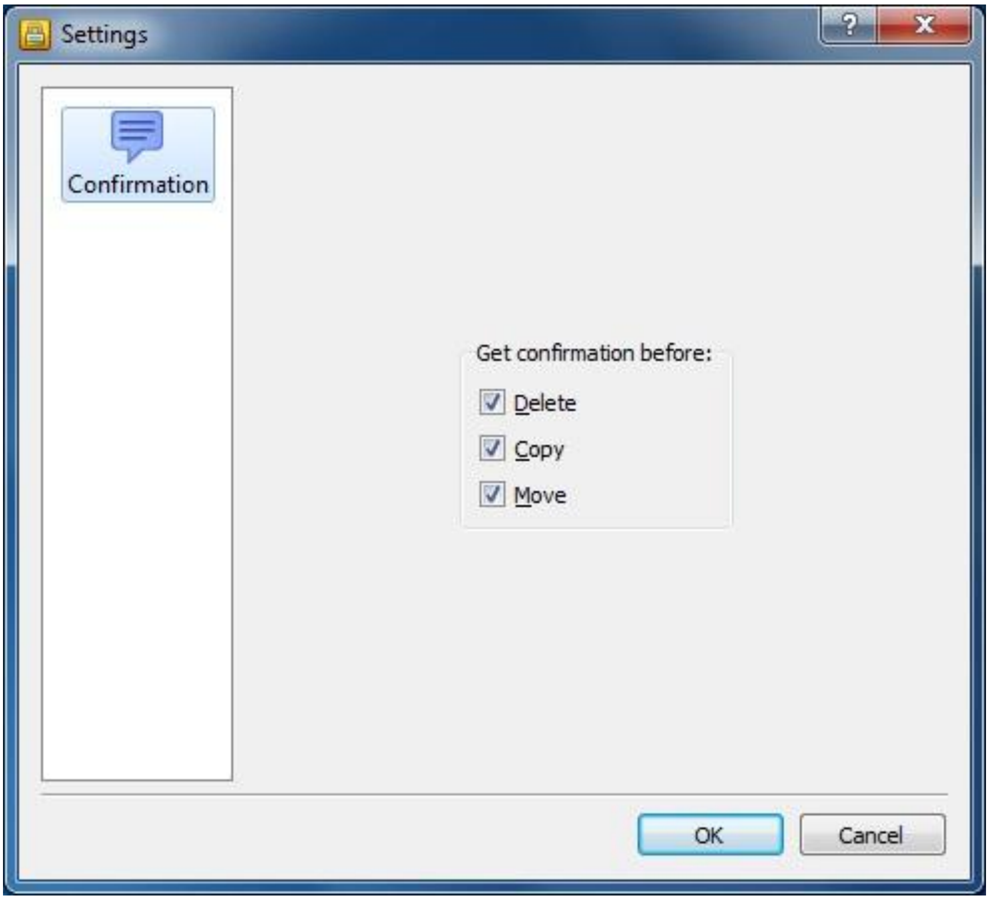
Mostrar imágenes de tipo árbol - para mostrar una estructura de árbol

Mostrar las imágenes detalladas - para mostrar informaciones adicionales sobre los archivos

Mostrar imágenes de tipo lista - para mostrar los elementos en una lista

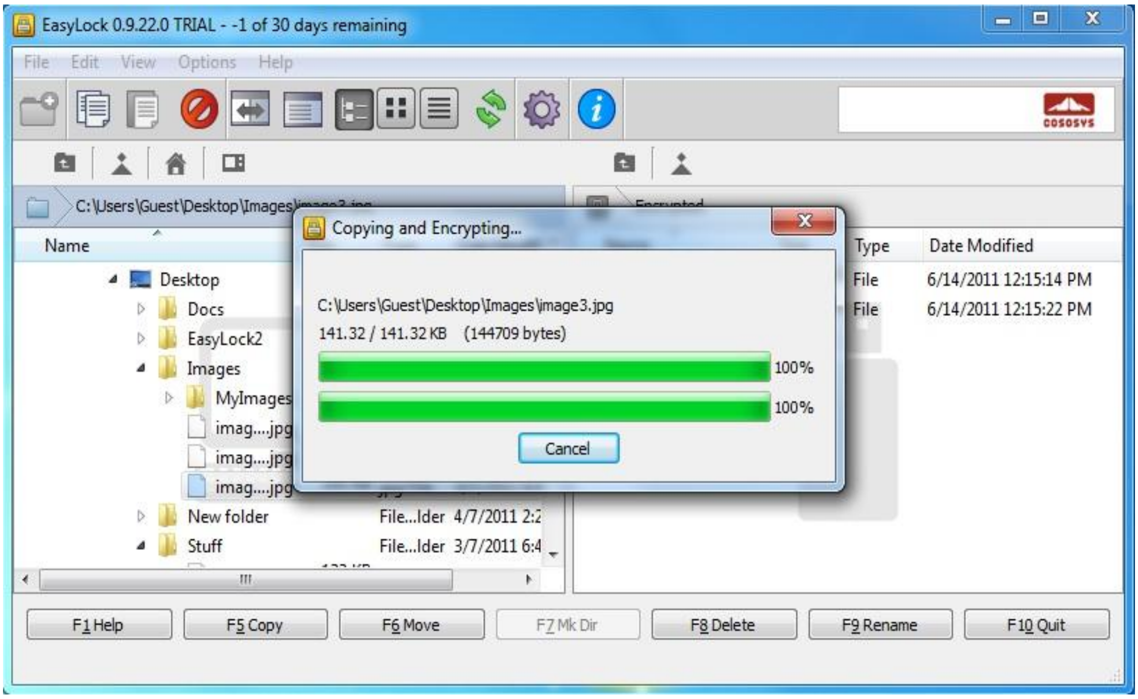
Las opciones disponibles también pueden ser seleccionadas directamente desde el menú principal en la sección Vista.

Puede seleccionar si desea mostrar un mensaje de confirmación antes de eliminar, copiar o mover archivos.

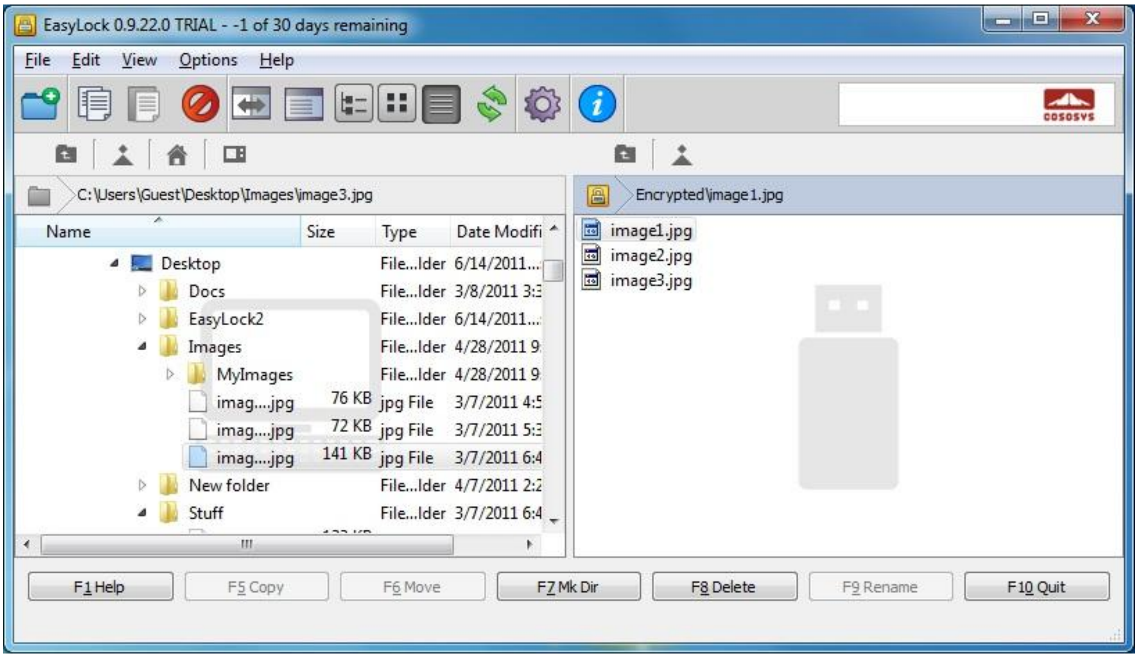


3.5. Utilizar la función de arrastrar y soltar para copiar archivos

Una función esencial de EasyLock es la función de arrastrar y soltar que le permite simplemente arrastrar el archivo/archivos y/o el directorio/directorios que desea copiar en el dispositivo y colocarlos en la ventana de EasyLock. Estos archivos serán encriptados automáticamente, asegurando que sus datos están seguros y se mantienen confidenciales.



El estado de encriptación y transferencia de archivos se puede observar con la barra de progreso. Cuando la barra llega al final, sus archivos han sido copiados y encriptados.



Si hace clic en un elemento con el botón derecho del mouse, tendrá acceso a otras opciones como “Actualizar”, “Copiar” y “Eliminar”.

Copiar archivos desde su disco duro al dispositivo de almacenamiento portátil utilizando Explorer **no es recommendable!**

Se recomienda utilizar la función de arrastrar y soltar o las teclas de método abreviado para copiar y pegar, Ctrl + C y Ctrl + V, para transferir datos a su dispositivo a través de la interfaz de EasyLock.

En la barra de herramientas de EasyLock, puede encontrar iconos adicionales que también se pueden utilizar para copiar y encriptar sus archivos.

Tenga en cuenta que los archivos de su dispositivo son visibles después de encriptación sólo si EasyLock esté en funcionamiento.

Para salir de EasyLock, seleccione el menú Archivo y seleccione Salida (Exit) o simplemente haga clic en la "X" en la esquina superior derecha de la ventana de la aplicación.

3.6. Abrir y modificar archivos en EasyLock

Los datos copiados en el dispositivo se pueden ver y editar directamente en EasyLock. Esta función está disponible con el comando "Abrir" o haciendo doble clic en el archivo deseado.

El usuario debe abrir los documentos en el dispositivo con la aplicación asociada. EasyLock tratará de cerrar estos documentos después de salir de la aplicación. Si un documento se modifica (y se guarda con la misma denominación, o incluso en el mismo directorio), este será encriptado y guardado en el dispositivo. Si un documento se modifica y se guarda, pero no se puede encriptar, por ejemplo, cuando se quita el dispositivo de forma inesperada, este será encriptado la próxima vez que usted inicie EasyLock.

ATENCIÓN! Cuando EasyLock es iniciado por Endpoint Protector como una aplicación de confianza, abrir documentos de la opción del dispositivo se desactiva porque la aplicación asociada no tiene acceso a los archivos.

3.7. Configuración de seguridad

La configuración de seguridad puede ser modificada en EasyLock. Después de la autenticación, puede cambiar su contraseña. En este sentido, debe acceder al menú de configuración de seguridad. Esto se puede hacer seleccionando Opciones -> Configuración de seguridad en la barra de herramientas o pulsando las teclas de método abreviado Ctrl + O.



4. Como funciona EasyLock con EPP o MyEPP

Cuando se utiliza EasyLock en un dispositivo de almacenamiento portátil, como TrustedDevice Level 1, en combinación con Endpoint Protector (o Mi Endpoint Protector con la solución alojada SaaS), se asegurará de que todos los datos copiados de un PC cliente protegido con Endpoint Protector al dispositivo se encriptarán.

Escenario normal para el uso de TrustedDevice Level 1 es el siguiente.

1. El usuario conecta el dispositivo al PC cliente protegido con Endpoint Protector.
2. El dispositivo es comprobado para la autorización (PC cliente se comunica con el servidor Endpoint Protector para verificar la autorización).
3. Si el dispositivo es un TrustedDevice Level 1 autorizado y el usuario o equipo es autorizado a utilizar el TrustedDevice Level 1, el software EasyLock en el dispositivo se abrirá automáticamente.
4. El usuario puede transferir archivos a través de arrastrar y soltar en EasyLock.
5. Los datos que se transfieren a los dispositivos son encriptados a través de AES de 256 bits.
6. El usuario no puede acceder al dispositivo directamente utilizando Windows Explorer o aplicaciones similares (por ejemplo, Total Commander) para asegurarse de que no se copian los datos en el dispositivo portátil sin estar debidamente encriptado.

7. El usuario no tiene la posibilidad de copiar datos en un estado desencriptado a TrustedDevice (en un PC cliente con Endpoint Protector).

8. Todas las transferencias de archivos desde un PC cliente con Endpoint Protector al dispositivo puede ser registrado si el rastreo de archivos y las sombras de archivos se activan en Endpoint Protector. Acciones tales como la eliminación de archivos o el cambio de nombre también se registran.

9. Los administradores pueden auditar más tarde cual usuario, con cual dispositivo, en cual PC, ha transferido los archivos.

Si un TrustedDevice no obtiene la autorización de Endpoint Protector, no se podrá utilizar por el usuario. El dispositivo se bloquea y el usuario no podrá acceder al dispositivo.

4.1. El seguimiento de archivos en EasyLock TrustedDevice

El seguimiento de archivos en EasyLock TrustedDevice es una nueva característica de Endpoint Protector 4 usada en combinación con EasyLock que permite el control de los archivos copiados de forma encriptada en dispositivos portátiles.

Al activar la opción de seguimiento de archivos, todos los datos transferidos hacia y desde dispositivos usando EasyLock se registran para el control posterior. La información registrada es enviada automáticamente al servidor Endpoint Protector si el cliente Endpoint Protector está presente en ese equipo y hay una conexión a Internet funcional.

En el caso de que el cliente Endpoint Protector no está presente, la información se almacena localmente en un formato encriptado en el dispositivo y será enviada en un momento posterior de cualquier otro equipo con el cliente Endpoint Protector instalado.

Para más detalles sobre la activación y el uso del seguimiento de archivos en EasyLock TrustedDevice, por favor consulte el Manual del usuario Endpoint Protector 4

Observación

La función de seguimiento de archivos en EasyLock TrustedDevices está disponible por el momento sólo para Windows OS.

5. Configurar el uso de TrustedDevice en EPP o MyEPP

Para saber cómo configurar el uso de TrustedDevice en combinación con Endpoint Protector, por favor consulte el Manual del Usuario Endpoint Protector.

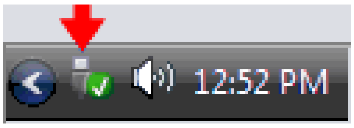
Para obtener más información sobre Endpoint Protector, visite: www.EndpointProtector.com

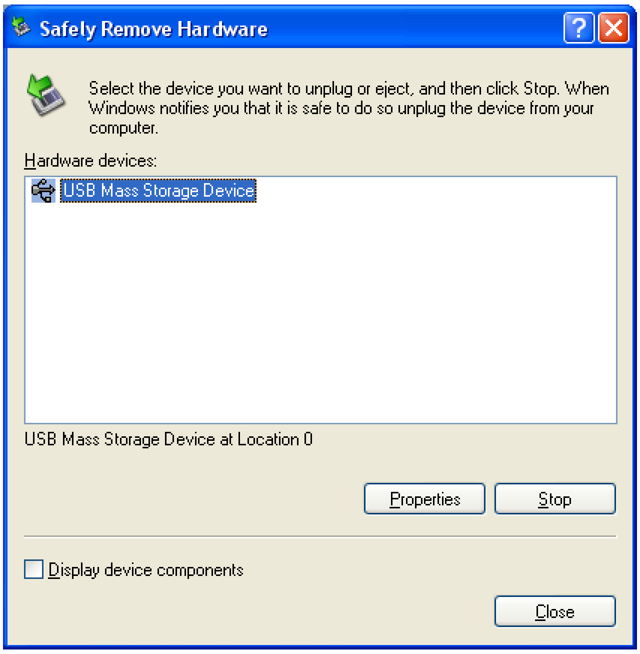
6. Quitar hardware de forma segura

Antes de desconectar el dispositivo de almacenamiento portátil desde el puerto USB de su computadora, usted tiene que utilizar la opción "Quitar hardware de forma segura" desde la bandeja del sistema, de lo contrario corre el riesgo de dañar los datos en su unidad USB.

Para quitar hardware de forma segura, haga doble clic en el icono de la bandeja del sistema, a continuación, seleccione la unidad USB que desea eliminar de la lista y haga clic en el botón "Stop".







Aparecerá un mensaje indicando que el dispositivo de almacenamiento portátil puede ahora ser eliminado de forma segura. Si aparece un mensaje diciendo: "The '…' device cannot be stopped right now" ("El '...' dispositivo no se puede detener ahora mismo"), usted tiene que cerrar Windows Explorer, EasyLock o cualquier otra aplicación que tenga todavía acceso a los datos en la unidad USB.

7. Soporte técnico

Si necesita soporte técnico adicional, tales como las preguntas frecuentes o asistencia por correo electrónico, se puede visitar página de Internet de soporte directamente en http://www.cososys.com/help.html

8. Aviso Importante / Descargo de responsabilidad

Las medidas de seguridad, por su naturaleza, pueden ser eludidas. CoSoSys no puede y no garantiza que los datos o los dispositivos no sean accedidos por personas no autorizadas, y CoSoSys renuncia a cualquier garantía en ese sentido a la mayor medida permitida por la ley.